在Catalyst 9800上使用錨點配置中央Web驗證

目錄

簡介 必要條件 需求 採用元件 配置錨定到其他Catalyst 9800的Catalyst 9800 網路圖表 在兩台9800上配置AAA 在WLC上配置WLAN 在外部WLC上建立策略配置檔案和策略標籤 在錨點WLC上建立策略配置檔案 重新導向兩台9800上的ACL設定 配置ISE 設定錨點到AireOS WLC的Catalyst 9800 Catalyst 9800外部配置 錨點AireOS WLC上的AAA配置 AireOS WLC上的WLAN配置 在AireOS WLC上重定向ACL 配置ISE 當AireOS WLC是外部, Catalyst 9800是錨點時, 配置的差異 驗證 疑難排解 Catalyst 9800故障排除資訊 客戶端詳細資訊 內嵌式封包擷取 RadioActive跟蹤 AireOS故障排除資訊 客戶端詳細資訊 從CLI調試 參考資料

簡介

本檔案介紹如何在Catalyst 9800上設定和疑難排解中央Web驗證(CWA),該驗證指向另一個無線 LAN控制器(WLC)作為行動錨點,且使用AireOS或其他9800 WLC覆蓋目的地。

必要條件

需求

建議您瞭解9800 WLC、AireOS WLC和Cisco ISE的基本知識。假設在啟動CWA錨點設定之前,您

已經開啟了兩個WLC之間的行動通道。超出此組態範例的範圍。如需相關幫助,請參閱標題為「<u>在</u> Catalyst 9800控制器上建立行動通道」的文件

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

9800 17.2.1

5520 8.5.164 IRCM映像

ISE 2.4

配置錨定到其他Catalyst 9800的Catalyst 9800

網路圖表



在兩台9800上配置AAA

在錨點和外部上,您需要先新增RADIUS伺服器並確保已啟用CoA。這可以在選單中完成 Configuration>Security>AAA>Servers/Groups>Servers>**單擊**Add按鈕

Cisco Cisco Ca	atalyst 9800-L Wireless Controller		Welcome admin Last login Fri, May 15 2020 16:56:51
Q Search Menu Items	Configuration * > Security * > AAA		
Dashboard	+ AAA Wizard		
Monitoring ;	Servers / Groups AAA Method Lis	st AAA Advanced	
	RADIUS	Servers Server Groups	
C Licensing	TACACS+		Austr Dans
X Troubleshooting	LDAP	Name Address	 Auth Port
	Create AAA Radius Server		×
	Name*	CLUS-Server	
	Server Address*	XXXX	
	PAC Key		
	Кеу Туре	Clear Text	
	Key*	••••••	
	Confirm Key*		
	Auth Port	1812	
	Acct Port	1813	
	Server Timeout (seconds)	1-1000	
	Retry Count	0-100	
	Support for CoA	ENABLED	
	つ Cancel		Apply to Device

現在需要建立伺服器組,並將剛才配置的伺服器放入該組中。此操作在 Configuration>Security>AAA>Servers/Groups>Server Groups>+Add處完成。

Cisco Cata	alyst 9800-L Wireless Co	ontroller	
Q Search Menu Items	Configuration > Security	y* > AAA	
📻 Dashboard	+ AAA Wizard		
Monitoring >	Servers / Groups AAA	Method List AAA Advanced	
Configuration	+ Add × Delete		
Administration	RADIUS	Servers Server Groups	
C Licensing	TACACS+	Nome	
💥 Troubleshooting	LDAP		 ✓. Ser
	Create AAA Radius Serve		^
	Name*	CLUS-Server-Group	
	Group Type	RADIUS	
	MAC-Delimiter	none 🔻	
	MAC-Filtering	none 🔻	
	Dead-Time (mins)	1-1440	
	Available Servers	Assigned Servers	
		CLUS-Server	
	Cancel	Apply to	Device

現在,建立一個**authorization**方法清單(對於CWA不需要身份驗證方法清單),其中型別為網路,組型別為組。將上一個 操作中的伺服器組新增到此方法清單中。

此配置在此處完成Configuration>Security>AAA>Servers/AAA Method List>Authorization>+Add

Cisco Catal	yst 9800-L Wirele	ess Controller			
Q Search Menu Items	Configuration > S	Security * > AAA			
📻 Dashboard	+ AAA Wizard				
Monitoring >	Servers / Groups	AAA Method List	AAA Advanced		
Configuration	Authentication				
Administration	Authorization	Ľ	+ Add × D		
© Licensing	Accounting Quick Setup: AAA	Authorization	Name	√ Туре	Group Type
X Troubleshooting	Method List Name*	CLUS-Au	thZ-Meth-List		
	Туре*	network	•		
	Group Type	group	•		
	Fallback to local				
	Authenticated				
	Available Server Groups	3	Assigned Server Group	ps	
	radius Idap	*	CLUS-Server-G	iroup 🔺	~
	tacacs+ ISE1	<			^
		»			▼
		*		-	<u>×</u>
	Cancel				Apply to Device

(可選)使用與授權方法清單相同的伺服器組建立記帳方法清單。可以在以下位置建立記帳清單 :Configuration>Security>AAA>Servers/AAA Method List>Accounting>+Add

Cisco Cata	lyst 9800-L Wirele	ess Controller				
Q Search Menu Items	Configuration * > S	Security * > AAA				
Dashboard	+ AAA Wizard					
G Monitoring >	Servers / Groups	AAA Method List	AAA Advanced			
Configuration	Authentication	ſ				
Administration >	Authorization		Name	V Type		Group1
C Licensing	Quick Setup: AAA	Accounting	Hume	1300		*
K Troubleshooting	Method List Name*	CLUS-	Acct-Meth-List			
	Туре*	identity	,			
	Available Server Groups	5	Assigned Server Gro	oups		
	radius Idap tacacs+ ISE1		CLUS-Serve	er-Group	× × × ×	
	Cancel				Apply to	Device

在WLC上配置WLAN

在兩台WLC上建立和配置WLAN。兩者上的WLAN應該相符。安全型別應為mac過濾,並應應用上 一步中的授權方法清單。此組態在Configuration>Tags & Profiles>WLANs>+Add下完成

Cisco Cat	alyst 9800-L Wireless	s Controller			
Q Search Menu Items	Configuration > Tag	s & Profiles * > WLANs			
Dashboard	+ Add × Dela				
Monitoring >	Number of WLANs selected	: 0			
Configuration	Add WLAN	e	v ID		× ×
	General Security	Advanced			
C Licensing	Profile Name*	CLUS-WLAN-Name	Radio Policy	All	J
X Troubleshooting	SSID*	CLUS-SSID	Broadcast SSID	ENABLED	
	WLAN ID*	2			
	Status				
	Cancel				Apply to Device

Cisco Cata	alyst 9800-L Wireless Controller	
Q Search Menu Items	Configuration * > Tags & Profiles * > WLANs	
Dashboard	+ Add × Delete Enable WLAN Disable WLAN	
Monitoring >	Number of WLANs selected : 0	
	Add WLAN	×
	General Security Advanced	
C Licensing	Layer2 Layer3 AAA	
X Troubleshooting	Layer 2 Security Mode None Lobby Admin Access	
	Authorization List*	
	Cancel	

在外部WLC上建立策略配置檔案和策略標籤

要建立策略配置檔案,請轉到**配置>標籤和配置檔案>策略>+新增**

錨定時,必須使用中心交換。

Cisco Catalys	st 9800-L Wireless Contr	roller		
Q Search Menu Items	Configuration * > Tags & Prof	files > Policy		
🔜 Dashboard	+ Add × Delete			
C Monitoring	Status V Policy Profile N	Name		 Description
Configuration	ad Policy Profile	QOS and AVC Mobility	Advanced	×
() Administration	A Confermin	a is spabled state will result is loss of a	encetivity for allegate consoleted with	this profile
C Licensing	A Coniguni	ig in enabled state will result in loss of co	onnectivity for clients associated with	unis prome.
X Troubleshooting	Name*	CLUS-Policy-Profile	WLAN Switching Policy	
	Description	Policy Profile for CLUS	Central Switching	
	Status		Central Authentication	
	Passive Client	DISABLED	Central DHCP	
	Encrypted Traffic Analytics	DISABLED	Central Association	
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging			
	SGACL Enforcement			
	Default SGT	2-65519		
	Cancel			Apply to Device

在「高級」頁籤上,CWA必須使用AAA覆蓋和RADIUS NAC。如果您選擇建立會計方法清單,還可 以在此處應用該清單。

Q Search Menu Items	Configuration > Tags & Pro	ofiles* > Policy		
🔜 Dashboard	+ Add × Delete			
Monitoring >	Status v Policy Profile	Name	~	Description
	Add Policy Profile			×
Configuration >	General Access Policies	QOS and AVC Mobility	Advanced	
Administration	WLAN Timeout		Fabric Profile Search or Select	Y
C Licensing	Session Timeout (sec)	1800	mDNS Service Search or Select Policy	•
💥 Troubleshooting	Idle Timeout (sec)	300	Hotspot Server Search or Select	•
	Idle Threshold (bytes)	0	User Private Network	
	Client Exclusion Timeout (sec)	60	Status	
	Guest LAN Session Timeout		Drop Unicast	
	DHCP		Umbrella	
	IPv4 DHCP Required		Umbrella Parameter Map	Clear
	DHCP Server IP Address Show more >>>		Flex DHCP Option For DNS	
	AAA Policy		DNS Traffic Redirect IGNORE	
	Allow AAA Override		WLAN Flex Policy	
	NAC State		VLAN Central Switching	
	NAC Type	RADIUS	Split MAC ACL Search or Select	•
	Policy Name	default-aaa-policy x	Air Time Fairness Policies	
	Accounting List	CLUS-Acct-Meth-	2.4 GHz Policy Search or Select	•

在「Mobility」索引標籤上,**請勿勾選「export anchor」覈取方塊,而是將錨點WLC新增到錨點清 單中。**確保點選「應用到裝置」。 請注意,此假設兩個控制器之間已建立行動通道

Cisco Cisco Cata	lyst 9800-L Wireless Controller			
Q. Search Menu Iteme	Configuration * > Tags & Profiles * >	Policy		
Dashboard	+ Add × Delete			
(2) Monitoring >	Add Policy Profile			×
Configuration	General Access Policies QOS a	IND AVC Mobility	Advanced	
203 Administration	Mobility Anchors			
C Licensing	Export Anchor			
Traubleshadting	Static IP Mookey Adding Mobility Anchors will cause the enabled disable and may result in basi of connectivity & Drag and Drop/double click/click on the am	I WLANs to momentarily r warme clients.		
	Available (0)	Selected (1)		
	Anchor IP	Anchor IP	Anchor Priority	
	No anchors available	192.168.160.18	Primary (1)	• •
	D Cancel			Apply to Device

為了讓AP使用此策略配置檔案,您需要建立策略標籤並將其應用到要使用的AP。

要建立策略標籤,請轉至Configuration>Tags & Profiles>Tags?Policy>+Add

Cisco Cata	alyst 9800-L Wirele	ss Controller		
Q Search Menu Items	Configuration • > Ta	ags & Profiles * > Tags		
Dashboard	Policy Site	RF AP		
Monitoring >	+ Add ×			
Configuration	Policy Tag Na	ame		
	Add Policy Tag			×
O Administration	Name*	CLUS-Policy-Tag		
C Licensing	Description	Delieu Teo for CLUS		
G Troubloobacting	Description	Policy Tag for CLUS		
Troubleshooting	V WLAN-POLIC	Y Maps: 0		
	+ Add × De	lete		
	WLAN Profile		 Policy Profile 	~
	4 4 0 ⊨ ⊨	10 🔻 items per page		No items to display
	Map WLAN and Po	licy		
	WLAN Profile*	CLUS-WLAN-Name	Policy Profile*	CLUS-Policy-Profile
	RLAN-POLICY	/ Maps: 0		
	Cancel			Apply to Device

要同時將此項新增到多個AP,請轉到**配置>無線設定>高級>立即開始**。點選「標籤AP」旁邊的專案 符號欄,將該標籤新增到您選擇的AP。

¢	dialia cisco	Cisco Cat	alyst 9800-L Wire	eless Controller								
٩	Search Menu Ite	ims	Configuration * >	Wireless Setup *	> Advance	ed						
	Dashboard		Start		«		- Tag APs					
	Monitoring			Tags & Profiles		Numb	er of APs: 3 ted Number o	of APs: 3				
Z			0	WLAN Profile	+		AP Name	~	AP Model ~	AP MAC ~	AP ~ Mode	4 5
ැබු	Administratio		0	Policy Profile	+		Jays2800		AIR-AP28021- B-K9	002a.10f3.6b60	Local	E
0	Licensing		0	Policy Tag 🛛 🥥	+		Jays3800		AIR-AP3802I- B-K9	70b3.1755.0520	Local	E
							AP0062.ec2	20.122c	AIR-CAP2702I- B-K9	cc16.7e6c.3cf0	Local	D
X	Troubleshoot		0	AP Join Profile	+	14	< 1 ∣		10 🔻 items per			
			0	Flex Profile	+	Tag	APs					×
			0	Site Tag 🛛 🥔	i= +	Та	gs					Į
						Po	licy	CLUS	-Policy-Tag 🗸			
			0	RF Profile	+	Sit	е	Search	h or Select 🔻			
			Ø	RF Tag 🧳	+	RF		Search	h or Select 🔻			
				Apply		Cł	anging AP Ta	g(s) will d	cause associated A	P(s) to reconnect		
			8	Tag APs			Cancel				to Device	
			Done									

在錨點WLC上建立策略配置檔案

前往錨點WLC Web UI。在錨點9800上**Configuration**>Tags & Profiles>**Tags>Policy>+Add下新增策略配置檔案**。確保此配 置與外部裝置上的策略配置檔案相匹配,移動頁籤和記帳清單除外。

此處不新增錨點,但會勾選「匯出錨點」覈取方塊。請勿在此處新增記帳清單。請注意,此假設兩個控制器之間已建立行 動通道

附註:沒有理由在策略標籤中將此配置檔案關聯到WLAN。如果您這樣做,將會出現問題。如果您想對此WLC上的AP使用 相同的WLAN,請為其建立另一個原則設定檔。

Cisco Catalyst 9800-L. Wireless Controller								
Q Search Menu Items Configuration * > Tags & Profiles * >	Policy							
Dashboard + Add × Delete								
Monitoring Add Policy Profile			×					
General Access Policies QOS and	d AVC Mobility Ad	dvanced						
Mobility Anchors Administration >								
C Licensing								
Static IP Mobility Image: Static IP Mobility Adding Mobility Anchors will cause the enabled will disable and may result in loss of connectivity for stable and Drag and Drop/double click/click on the arrow	Static IP Mobility DISABLED bleshooting Adding Mobility Anchors will cause the enabled WLANs to momentarily disable and may result in loss of connectivity for some clients. Drag and Drop/double click/click on the arrow to add/remove Appropriate Approprise Approprise Appropriate Appropriate Approprise Appropr							
Available (1)	Selected (0)							
Anchor IP	Anchor IP	Anchor Priority	_					
≤ 192.168.160.16		Anchors not assigned						
Cancel			ply to Device					

重新導向兩台9800上的ACL設定

接下來,您需要在兩台9800上建立重新導向ACL組態。外部的條目並不重要,因為它是將ACL應用於流量的錨點WLC。唯 一的要求是它在那裡,並且有一些條目。錨點上的條目必須「拒絕」埠8443上的ISE訪問,並且「允許」所有其他內容。 此ACL僅適用於從客戶端「進入」的流量,因此不需要返回流量的規則。DHCP和DNS將在ACL中無條目的情況下通過。

Cisco Cata	alyst 9800-L Wireless Co	ontroller			Welcome admin
Q Search Menu Items	Configuration * > Security	> ACL			
Dashboard	+ Add × Delete Add ACL Setup	Associate Interfaces			×
Monitoring >	ACL Name*	CLUS-ACL	ACL Type	IPv4 Extended	
Configuration	Rules				
() Administration	Sequence*		Action	permit v	
© Licensing	Source Type	any 🔻			
X Troubleshooting	Destination Type	any 🔻			
	Protocol	ahp 🔻			
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence ~ Action	 Source ~ Source ~ IP Wildcard 	Destination ~ Destination ~ Wildcard	Protocol v Port	Destination ~ Port DSCP ~ Log ~
	D 10 deny	any	192.168.160.99	tcp None	eq 8443 None Disabled
	100 permit	any	any	ip None	None None Disabled
		10 🔻 items per page			1 - 2 of 2 items
	Cancel				Apply to Device

配置ISE

最後一步是為CWA配置ISE。此方式有很多選項,但本示例將堅持基本並使用預設的自註冊訪客門 戶。

在ISE上,您需要建立授權配置檔案、帶有身份驗證策略的策略集和使用授權配置檔案的授權策略 ,將9800(外部)作為網路裝置新增到ISE,並建立使用者名稱和密碼以登入網路。

要建立授權配置檔案,請轉至Policy>Policy Elements>Authorization>Results>Authorization Profiles>,然後按一下Add。確保返回的訪問型別為「access_accept」,然後設定要傳送回的 AVP(屬性 — 值對)。對於CWA,重定向ACL和重定向URL是必需的,但您也可以傳送回諸如 VLAN ID和會話超時等內容。非常重要,ACL名稱應與外部和錨點9800上的重新導向ACL名稱相匹 配。

$\epsilon \rightarrow C$ A Not secure 19	2.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions_authorization/policy_element
dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers
Policy Sets Profiling Posture Cl	ent Provisioning Policy Elements
Dictionaries Conditions Result	
Authentication Authorization Authorization Profiles Downloadable ACLs Profiling Posture Client Provisioning	Authorization Profiles > test Authorization Profile * Name CLUS-AuthZ-Profile-ISE Description * Access Type ACCESS_ACCEPT Network Device Profile @@Cisco U Service Template Track Movement () Passive Identity Tracking ()
	✓ Common Tasks Voice Domain Permission Web Redirection (CWA, MDM, NSP, CPP) () Centralized Web Auth ▼ ACL CLUS-ACL Value Self-Registered Guest Portal (c▼

然後,您需要配置一種方法,將剛剛建立的授權配置檔案應用到通過CWA的客戶端。為此,一種方 法是建立在使用MAB時繞過身份驗證的策略集,並在使用被叫站ID中傳送的SSID時應用授權配置檔 案。同樣,有很多方法可以實現這一點,因此,如果您需要一些更具體或更安全的方法,這是最簡 單的方法。

要建立策略集,請轉至**Policy>Policy Sets**,然後點選螢幕左側的+按鈕。命名新策略集,並確保將 其設定為「預設網路訪問」或允許對MAB進行「進程主機查詢」的任何允許的協定清單(要檢查允 許的協定清單,請轉至Policy>Policy Elements>Results>Authentication>Allowed Protocols)。 現 在點選您建立的新策略集中間的+符號。

-shude. Identify Services Engine Home + Context Visibility + Operat	ons Policy + Administration + Work Centers		License Warning 🔺 🔍 🛛 🔿 🔿
Policy Sets Profiling Posture Client Provisioning Policy Elements			Click here to do visibility setup Do not show this again.
Policy Sets			ResetAll Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions		Allowed Protocols / Server Sequence Hits Actions View
Search			
O CLUS CWA-Policy-Set		+	Default Network Access 🔹 🔹 +
Default Default Default			Default Network Access * * + 0 🌣 >
			Reset

對於此策略設定,每次在ISE中使用MAB時,它將通過此策略設定。稍後,您可以制定與被叫站 ID匹配的授權策略,以便根據使用的WLAN應用不同的結果。此流程非常可定製,可以匹配許多內 容。

Conditions Studio		
Library	Editor	
mab ♥ ⊑ □ ▲ ⊕ 및 빌 함 ऌ ዸ ፟ ፟ © ↓ ♥ ఓ 奈	Wireless_MAB Set to 'Is not'	0
Wired_MAB ()		
Uireless_MAB	+ New AND OR	

在策略集中,建立策略。身份驗證策略可以在MAB上再次匹配,但您需要更改ID儲存以使用「內部 端點」,並且需要更改選項以繼續身份驗證失敗且找不到使用者。

Policy Sets Profiling Posture Client Provisioning + Policy Elements	Click here to do visibility setup Do not show this again.
Policy Sets + CLUS-CWA-Policy-Set	ResetAll Hitcounts Reset Save
Status Policy Set Name Description Conditions	Allowed Protocols / Server Sequence Hits
Search	
CLUS-CWA-Policy-Set	Default Network Access * * • •
▼Authentication Policy (2)	
Status Rule Name Conditions	Use Hits Actions
O OULSAME Condition	Internal Endopints • • ♥ Options If Auth fail CONTINUE • • If User not found • • CONTINUE • • If Process fail DROP
O Default	Al_User_I0_Stores * * ► Options 0 \$
Authorization Policy - Local Exceptions	
Authorization Policy - Global Exceptions	
Authorization Policy (1)	

設定身份驗證策略後,需要在授權策略中建立兩個規則。此策略看上去像ACL,因此順序需要將 post-auth規則放在頂部,將pre-auth規則放在底部。後身份驗證規則將匹配已通過訪客流的使用者 。也就是說,如果他們已經登入,他們將遵循該規則並停止。如果他們尚未登入,則會繼續下清單 並點選獲取重定向的預身份驗證規則。最好將授權策略規則與以SSID結尾的被叫站ID相匹配,以便 僅對配置為這樣做的WLAN進行命中。

Policy	Sets 🗕	CLUS-CWA-Policy-Set							ResetAll Hitcounts
	Status	Policy Set Name	Descrip	ption	Cond	titions			Allowed Protocols / Server
Search									
	0	CLUS-CWA-Policy-Set				Wireless_MAB			Default Network Access
> Auth	entication	n Policy (2)							
> Auth	orization	Policy - Local Exceptions							
> Auth	orization	Policy - Global Exceptions							
♥ Auth	orization	Policy (4)							
(+) Searc	Status	Rule Name	Cond	itions			Results Profiles	Security	Groups
$\left[\right]$	ø	Post-CWA	AND	E Network Access	-UseCa Station-II	se EQUALS Guest Flow O ENDS_WITH CLUS-SSID	CLUS-Post-Auth	+ Select f	om list 🔹 🕇
	ø	MAB on WLAN	AND	Radius-Called-	Station-II	D END\$_WITH CLUS-SSID	× CLUS-Auth2-Profile-ISE	+ Select 1	rom list 🔹 🕇
	0	Flex AuthZ	무	Radius Called-Station-ID	ENDS_	WITH FLEX-CWA	× CLUS-Flex_CWA	+ Select f	rom list 👻 🕇
	ø	Default					× DenyAccess	+ Select f	rom list 👻 🕇

現在策略集已配置,您需要通知ISE關於9800(外部),以便ISE將其信任為身份驗證器。這可以在 Admin>Network Resources>Network Device>+中執行。您需要為其命名、設定IP地址(在本例中 為整個管理子網)、啟用RADIUS並設定共用金鑰。ISE上的共用金鑰必須與9800上的共用金鑰匹 配,否則此進程將失敗。新增配置後,按一下「提交」按鈕儲存配置。

dentity Services Engine	Home Context Visibility Operations Policy Administration Work Centers	
System Identity Management		
Network Devices Network Device	Sroups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services	
Network Devices Default Device Device Security Settings	Network Devices List > JAysNet Network Devices * Name CLUS_Net-Device Description	
	IP Address v * IP : 192.168.160.0 / 24	
	* Device Profile Model Name Model Name	
	IPSEC No Set To Default	
	Device Type All Device Types Set To Default Image: Constraint of the set	
	Protocol RADIUS Shared Secret Show Use Second Shared Secret G CoA Port 1700 Set To Default RADIUS DTLS Settings ()	

最後,您需要將客戶端要輸入的使用者名稱和密碼新增到登入頁面,以驗證他們是否有權訪問網路 。此操作在Admin>Identity Management>Identity>Users>+Add下完成,並確保在新增後按 submit。 與ISE的所有其他配置一樣,這是可自定義的,無需使用者本地儲存,但也是最簡單的配 置。

cisco	Identity Service	es Engine	Home 🕨	Context Visibility	Operations	▶ Policy	✓ Adminis	stration > Wo	rk Centers	
► Sy	stem 🔽 Identity	Management	Network Reso	ources + Devic	e Portal Manageme	nt pxGrid	Services •	Feed Service	Threat Centric NAC	
▼ Ide	ntities Groups	External Identi	ty Sources Io	lentity Source Se	quences • Setting	js				
		G								
Users			Network Acc	ess Users List >	New Network Acces	s User				
Latest	Manual Network S	can Results	• Netwo	TR ACCESS USE	`					
			* Name	CLUS-User	J					
			Status	Enabled •						
			Email							
			▼ Pass	words						
			Passwo	ord Type: Inter	nal Users	Ŧ				
				Pass	word		Re-Enter Pas	ssword		
			* Loain	Password	•••		•••••		Generate Password	(i)
			Enable	Password		'`			Generate Password	(i)
										•
			▼ User	Information						
			First Na	ame						
			Last Na	ame						
				unt Ontions						
			▼ Acco	unt Options						
				Des	cription					
			Change	e password on ne	xt login 🛛					
			▼ Acco	unt Disable Po	licy					
				sable account if d	ate exceeds 2020	-07-17		(vvvv-mm-d	1)	
					2020	07-17		())))	~/	
			▼ User	Groups						
			Select	an item	0					
			Submit	Cancel						

設定錨點到AireOS WLC的Catalyst 9800



Catalyst 9800外部配置

按照前面討論的步驟操作,跳過「在錨*點WLC上建立策略配置檔案*」部分。

錨點AireOS WLC上的AAA配置

前往**Security>AAA>RADIUS>Authentication>New**,將伺服器新增到WLC。新增伺服器IP地址、共 用金鑰和支援CoA。



AireOS WLC上的WLAN配置

若要建立WLAN,請轉至WLANs>Create New>Go。

配置配置檔名稱、WLAN ID和SSID,然後點選「Apply」。

،،ا،،،ا،، cısco		ANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK		
WLANs	WLANs									
VLANs	Current Filter:	None	[Change Filte	r] [Clear Filter	1				Create New 🗸	Go
Advanced		ype Profile Name W	LAN SSID A	dmin Status	Security Policies					
IIIIIII CISCO MONT	R WLANS CONTROLLER WIS	RELESS SECURITY MANAGEM	ENT COMMANDS	HELP EEEDBACK					Sage Configuration Ping Logo	ut Befresh
WLANS WLAI	s > New								< Back	Apply
WLANS WLANS Advanced Type	Name CLUS-WLAP CLUS-WLAP CLUS-SSID 1	• N-Name								

這麼做應會進入無線區域網組態。在「General」頁籤上,如果您不打算配置ISE在AVP中傳送,您 可以新增希望客戶端使用的介面。接下來,前往**Security>Layer2**索引標籤,並匹配在9800上使用的 「Layer 2 Security」配置並啟用「MAC Filtering」。



現在移至**Security>AAA Servers**頁籤,並將ISE伺服器設定為「Authentication Servers」。**請勿為** 「記帳伺服器」設定任何內容。 取消選中「啟用」框以進行記帳。



仍處於WLAN配置中時,移至「Advanced」頁籤並啟用「Allow AAA Override」,並將「NAC State」更改為「ISE NAC」

ll cisco	MONITOR WLANS CONTROLLER W	RELESS SECURITY MANAGEMENT COMMANDS	HELP FEEDBACK		Logout Befresh
WLANs	WLANs > Edit 'CLUS-WLAN-Nam	e'		< Back	Apply
VLANS	General Security QoS Po	licy-Mapping Advanced			
Advanced	Allow AAA Override Coverage Hole Detection Enable Session Timeout Ainonet IE Diagnotes Channel III Override Interface ACL Lawer2 Ad URL ACL P2P Blocking Action Clinet Exclusion 2 Maximum Allowed Clients 8 Satici FP Tumening III WirFr Direct Clients Piloy Maximum Cliente Alloy		DHCP DHCP Server DHCP Addi. Assignment PHCP Addi. Assignment DHCP Addi. Assignment Split Turnel Split Turnel Beabled Management Frame Protection (HFP) NHP Client Protection GOLINH Period (in beacon intervals) BOLINH Period (in beacon intervals) BOLINH (1 - 255) 1 BOLINH (1 - 255) 1 BOL		
	Clear HotSpot Configuration	Enabled	Load Balancing and Band Select		-

最後是把它固定在自己身上。若要執行此操作,請返回**WLANs**頁面,並懸停在WLAN>移動錨點右 側的藍色框上。將「Switch IP Address(Anchor)(交換機IP地址(錨點))」設定為「local」,然後 按下「Mobility Anchor Create」按鈕。隨後應顯示優先順序0為本地錨點。

،را،،را،، cısco		MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK			
WLANs		WLANs											
VLANs		Current Fill	ter: Nor	ne	[Change Filte	er] [Clear Filter	1				Create New	▼ Go	I
Advanced		U WLAN I	D Type	Profil	e Name		WLAN SSI	D		Admin Status	Security Policies		
			WLAN	CLUS-	WLAN-Name		CLUS-SSID			Enabled	MAC Filtering		Pamara
													Mobility Anchors
													S02.110
													Service
													Advertisements Hotspot 2.0
WLANs	Mobility	Anchors											< Back
* WLANS													
WLANs Advanced	WLAN SS	ID CLUS-SSID	_										
	Switch IP	Address (Anchor)								Up Data Path	Control Path up	0 Priority	
	Mobility	Anchor Create											
	Switch I	P Address (And	uor) II	2.168.160.18 ¥									
	Delegitu		,										
	Priority		3	<u> </u>									
	Foot Not	es											

在AireOS WLC上重定向ACL

這是AireOS WLC上所需的最終配置。若要建立重新導向ACL,請前往**Security>Access Control** Lists>Access Control Lists>New。輸入ACL名稱(該名稱必須與AVP中傳送的名稱匹配),然後點 選「Apply」。

ahaha		Sage Configuration Eing Logout Befresh
CISCO	Monitor Wlans Controller Wireless Security Management Commands Help Feedback	🕺 Home
Security	Access Control Lists > New	< Back Apply
AAA General RADIUS Authentication Accounting Palback DNS Downloaded AVP TACACS+	Access Control List Name CUUS-ACU ACL Type IPv4 OIPv6	

現在,按一下剛建立的ACL的名稱。按一下「新增新規則」按鈕。與AireOS WLC上的9800控制器 不同,您可以為允許到達ISE的流量配置允許語句,而無需重定向。 預設情況下允許DHCP和 DNS。

uluılu cısco	MONI	TOR	WLANs		۶ W	VIRELESS	SECURIT	r I	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK		Sa <u>v</u> e Co	nfiguration	<u>P</u> ing	Logout <u>R</u> ef	fre: om
Security	Acce	ess Co	ontrol	Lists > Edit										[< Back	A	dd New Rule	,
▼ AAA General ▼ RADIUS	Gene	eral																
Authentication Accounting Fallback DNS	Access Deny (s List Na Counter	s	CLUS-ACL 5														
Downloaded AVP	Seq	Actio	n So	urce IP/Mask		Destina	tion IP/Ma	sk	Protocol	Source Por	t	Dest Port	DSCP	Direction	Number	of Hits		
LDAP Local Net Users	ı	Permit	0.0	0.0.0 0.0.0	/	192.168. 255.255.	160.99 255.255	/	тср	Any		8443	Any	Any	273			
MAC Filtering Disabled Clients User Login Policies	2	Permit	19 25	2.168.160.99 5.255.255.255	/	0.0.0.0 0.0.0.0		/	тср	8443		Any	Any	Any	566			
AP Policies Password Policies	_																	
Local EAP																		
Advanced EAP																		
Priority Order																		
Certificate																		



Access Control Lists CPU Access Control

CWAISE

ISE9800ISE

Policy>Policy Elements>Authorization>Results>Authorization Profiles>+Addaccess_acceptAVP — CWAACLURLVLAN ID ACLWLCWLCACL

🗧 🔶 C 🔺 Not secure | 192.168.160.99/admin/#policy/policy_elements/policy_elements_permissions/policy_elements_permissions/authorization/policy_element

dentity Services Engine	Home	Operations	▼Policy	Administration	Work Centers
Policy Sets Profiling Posture C	lient Provisioning 🔽 Policy Elem	ents			
Dictionaries + Conditions	ts				
0					
Authentication	Authorization Profiles > test				
Contraction Contraction	Autionzation Prome		ad	Г	
 Authorization 	Name (LUS-AuthZ-Profile-1	58		
Authorization Profiles	Description				1
Downloadable ACLs	* Access Type	CCESS_ACCEPT	.		
▶ Profiling	Network Device Profile	🗠 Cisco 👻 🕀			
► Posture	Service Template)			
Client Provisioning	Track Movement) (i)			
	Passive Identity Tracking) ()			
	 Common Tasks 				
	Voice Domain Permission	on			
	Web Redirection (CWA)	, MDM, NSP, CPP)	<i>i</i>)		
	Centralized Web Auth	•	ACL	CLUS-ACL	Value Self-Registered Guest Portal (C -

CWAMABIDSSID

Policy>Policy Sets+MABPolicy>Policy Elements>Results>Authentication>Allowed Protocols +

denter Identity Services Engine Home + Context Visibility + Op	rations Policy + Administration + Work Centers	License Warning 🔺 🔍 😐 🔿 🔿
Policy Sets Profiling Posture Client Provisioning + Policy Elements		Click here to do visibility setup Do not show this again.
Policy Sets		ResetAll Hitcounts Reset Save
+ Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Search		
O CLUS CWA-Policy-Set	+	Default Network Access 🔹 👻 +
Default Default Default		Default Network Access ** + 0 🗘 🕨

ISEMABIDWLAN



MABID

Polcy Sets Profiling Posture Client Provisioning + Polcy Elements	Click here to do visibility setup Do not show this	again.	×
Policy Sets → CLUS-CWA-Policy-Set	ResetAll Hitcounts R	eset	Save
Status Policy Set Name Description Conditions	Allowed Protocols / Server Se	equence	Hits
(Beard)			
CLUS-CWA-Policy-Set	Default Network Access	+	0
Authentication Policy (2)			
Status Rule Name Conditions	Use	Hits	Actions
O O	Internal Endpoints		٥
Default	All_User_ID_Stores * * > Options	0	٥
Authorization Policy - Local Exceptions			
Authorization Policy - Global Exceptions Authorization Policy (1)			

ACLpost-authpre-authSSIDIDWLAN

Policy Sets + CLUS-CWA-Policy-Set

Policy c	Sets +	CLUS-GWA-Policy-Set									ResetAll Hite	counts	
	Status	Policy Set Name	Descrip	otion	Con	litions					Allowed Protoc	cols / Server S	
Search													
	0	CLUS-CWA-Policy-Set		Wreless_MAB									
> Authe	entication	n Policy (2)											
> Autho	orization	Policy - Local Exceptions											
> Autho	orization	Policy - Global Exceptions											
← Autho	orization	Policy (4)											
٠	Status	Rule Name	Condi	itions				Results Profiles Security Groups					
Search	h												
	0	Post-CWA	AND	E Network Acces	-UseCa Station-I	se EQUALS Guest Flow D ENDS_WITH CLUS-SSID			CLUS-Post-Auth	+	Select from list	· +	
	ø	MAB on WLAN	AND	Radius-Called-	Station-I	D ENDS_WITH CLUS-SSID			× CLUS-Auth2-Profile-ISE	+	Select from list	× +	
	ø	Flex AuthZ	₽	Radius Called-Station-IE	ENDS,	WITH FLEX-CWA			CLUS-Flex_CWA	+	Select from list	- +	
	ø	Default							× DenyAccess	+	Select from list	- +	

ISE9800ISEAdmin>Network Resources>Network Device>+.IPRADIUSISE9800

Admin>Identity Management>Identity>Users>+Add ISE

cisco	Identit	y Service	s Engine	Home	Context Visibility	y	▶ Policy	Administ	tration 🔷 Wo	ork Centers
► Sy	stem [- Identity I	Nanagement	Network R	tesources + De	vice Portal Manageme	nt pxGrid	Services +	Feed Service	Threat Centric NAC
✓ Ide	entities	Groups	External Identit	y Sources	Identity Source S	equences + Setting	js			
▼ Ide	Manual I	Groups	External Identit	y Sources Network Network Nar Stat Em Pas Lo Ena Us Firs Las Ac Cha Us Se	Identity Source S Access Users List work Access Users List ane CLUS-User US Enabled ail sswords sword Type: Inf gin Password ble Password t Name t Na	New Network Accesser > New Network Accesser > New Network Accesser ser	JS IS USER	Re-Enter Pas	ssword	d)
				Subm	Cancer					

當AireOS WLC是外部, Catalyst 9800是錨點時, 配置的差異

如果您希望AireOs WLC成為外部控制器,則配置與之前相同,只有兩個差異。

- 1. AAA記帳從來不在錨點上完成,因此9800沒有記帳方法清單,而AireOS WLC將啟用記帳並指 向ISE。
- 2. AireOS需要錨定到9800而不是其自身。在策略配置檔案中,9800不會選擇錨點,但會選中「 匯出錨點」框。
- 3. 必須注意的是,當AireOS WLC將使用者端匯出到9800時,並沒有原則設定檔的概念,只會傳送WLAN設定檔名稱。因此,9800會將從AireOS傳送的WLAN配置檔名稱應用到WLAN配置檔 名稱和策略配置檔名稱。這表示從AireOS WLC錨定到9800 WLC時,兩個WLC上的WLAN設 定檔名稱和9800上的原則設定檔名稱必須全部相符。

驗證

若要驗證9800 WLC上的組態,請執行命令

Show Run | section aaa|radius

• WLAN

Show wlan id <wlan id>

• 策略配置檔案

Show wireless profile policy detailed <profile name>

• 策略標籤

Show wireless tag policy detailed <policy tag name>

ACL

Show IP access-list <ACL name>

• 驗證使用錨點的移動性是否啟動

Show wireless mobility summary 要驗證AireOS WLC上的配置,請運行命令

AAA

Show radius summary 附註:RFC3576是CoA配置

• WLAN

Show WLAN <wlan id>

ACL

Show acl detailed <acl name>

•驗證與外部裝置的移動性是否正常

Show mobility summary

疑難排解

根據客戶端在該過程中停止的點,故障排除看起來不同。例如,如果WLC從未從MAB上的ISE收到 響應,則客戶端將停滯在「Policy Manager State:(策略管理器狀態:)」Associating」和「」 將不會匯出到錨點。在這種情況下,您只會對外來路由器進行疑難排解,可能會為WLC和ISE之間 的流量收集RA追蹤和封包擷取。另一個範例是MAB已成功通過,但使用者端沒有收到重新導向。在 這種情況下,您需要確保外部在AVP中收到重定向並將其應用於客戶端。您還需要檢查錨點,以確 保客戶端的正確ACL位於錨點上。此故障排除範圍超出本技術文檔的設計範圍(有關通用客戶端故 障排除指南的參考)。 如需更多有關在9800 WLC上排除CWA的幫助,請參閱Cisco Live!演示DGTL-TSCENT-404

Catalyst 9800故障排除資訊

客戶端詳細資訊

show wireless client mac-address 在此您應檢視「策略管理器狀態」、「會話管理器>身份驗證方法」、「移動角色」。

也可在GUI的「監控」(Monitoring)>「客戶端」(Clients)下找到此資訊

內嵌式封包擷取

在CLI中,命令啟動#monitor capture <capture name>,然後選項會在此後顯示。

在GUI上前往疑難排解>封包擷取>+Add

RadioActive跟蹤

在CLI上

debug wireless mac/ip

使用該命令的no形式將其停止。此檔案將記錄到bootflash中名為"ra_trace"的檔案中,然後記錄客戶 端的MAC或IP地址以及日期和時間。

在GUI上,轉到「Troubleshoot」>「Radiative Trace」>「Add」。新增客戶端的mac或ip地址,點 選apply,然後點選start。完成該過程數次後,停止跟蹤、生成日誌並將其下載到您的裝置。

AireOS故障排除資訊

客戶端詳細資訊

在CLI上show client details <client mac>

在GUI監視器>客戶端上

從CLI調試

Debug client

Debug mobility handoff

Debug mobility config



使用9800控制器構建移動隧道

9800上的無線調試和日誌收集